Reminder to Schools Using Federal Funds for Internet Connectivity

---

Schools using E-rate funds to pay for Internet access and other eligible services as defined by the Universal Service Administrative Company (USAC) which implements the E-rate funding program through the Federal Communication Commission (FCC) must certify compliance with the Children's Internet Protection Act (CIPA). This means the school is enforcing an internet safety policy that includes measures to block or filter internet access for both minors and adults to certain visual depictions. The basic CIPA requirements are outlined below. ***If there are questions about CIPA, the individual or organization used by a school to file for E-rate discounts should be consulted.***

CIPA requirements include three items:
1. Internet Safety Policy
2. Technology Protection Measure
3. Public Notice and Hearing or Meeting

1. Internet Safety Policy

Schools and libraries are required to adopt and enforce an internet safety policy that includes a technology protection measure that protects against access by adults and minors to visual depictions that are obscene, child pornography, or - with respect to use of computers with internet access by minors - harmful to minors. "Minor" is defined as any individual who is under the age of 17.This internet safety policy must address all of the following:

- Access by minors to inappropriate matter on the internet and World Wide Web;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Unauthorized access including "hacking" and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures designed to restrict minors' access to materials harmful to minors.
- For schools, the policy must also include monitoring the online activities of minors. As of July 1, 2012, as part of their CIPA certification, schools also certify that their internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

2. Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters internet access. CIPA uses the federal criminal definitions for obscenity and child pornography. The term "harmful to minors" is defined as "any picture, image, graphic image file, or other visual depiction that - (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual

contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors."

Decisions about what matter is inappropriate for minors are made by the local community. E-rate Program rules specify that "[a] determination regarding matter inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination."

3. Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. *For private schools, public notice means notice to their appropriate constituent group.*

Below is a list of the documentation that will be requested to demonstrate CIPA compliance during an audit. A school or library should retain copies of the documentation for each funding year where a CIPA certification is required. **Note that documents must be retained for at least 10 years after the latter of the last day of the applicable funding year or the service delivery deadline for the funding request.**

- A copy of the internet safety policy.
- Documentation that the school or library gave public notice and held a public hearing or meeting on the policy.
- For example, a school or library could demonstrate public notice with a copy of a website announcement for a regular school or library board meeting open to the public where the policy will be discussed, or an advertisement in a local newspaper of a county, government hearing or meeting where the policy appears as an agenda item. The school or library could also demonstrate that the hearing or meeting occurred with a copy of the minutes of the hearing or meeting and the date it occurred.
- Since 2011, entities have been required, at a minimum, to keep some record of when public notice was provided and when the hearing or meeting took place (e.g., a copy of the meeting agenda or a newspaper article announcing the hearing or meeting).
- Documentation of the adoption of the policy - for example, approval in the minutes of the hearing or meeting, or documented adoption by a school or library board.
- A description of the filter.
- A report or other documentation on the use of the filter.
- The documentation should show that the filter was installed and was working during the funding year. For example, a school that purchased filtered internet access could archive a sampling of reports from the service provider of internet sites blocked, or bills from the service provider verifying that the filter was operational. If a school purchased its own filter, it could archive logs produced by its IT staff showing the hours the filter was engaged.
- Copies of the FCC Form 479 and/or FCC Forms 486, as applicable.